REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated June 3, 2005. Claims 1-87 are pending. Claims 1, 5, 37, 41, 73, and 77 have been amended. Claims 4, 7-8, 9-36, 40, 43-72, 76, and 79-87 have been canceled. Accordingly, claims 1-3, 5-6, 37-39, 41-42, 73-75, and 77-78 remain pending in the present application.

Specification

Per the Examiner's request, the Title of the invention has been amended to "Hashing Algorithm Used for Multiple Files Having Identical Content and Fingerprint ID in a Peer-To-Peer Network."

Claim Objections and Rejections

The Examiner objected to claims 3, 39 and 75 for reciting "SHA1" instead of "SHA". However, Page 9 of the Specification states that "Keyed SHA1" is an example of fingerprinting or hash code algorithm that may be used in conjunction with the technique of the present invention, as described in RFC 2841 (attached to the application as Appendix B). RFC 2841 specifies a newer version of SHA than that described in [FIPS-180], which was flawed. Hence, the name Keyed SHA1. Therefore, the use of the name "SHA1" is correct.

The typographical errors in claims 8, 37 and 80 pointed out by the Examiner have been correct by cancellation or amendment, as suggested.

The Examiner rejected claims 1, 37 and 73 under 35 USC §112, second paragraph, for failing to have proper antecedent basis for the phrases "the other peer

devices", and "<u>the</u> content of the first information file." In response, the phrase "the

other peer devices" has been amended to recite "other peer devices." As for the

phrase "<u>the</u> content of the first information file," it is respectfully submitted that the term

"content" appears in the preamble of claims 1, 37 and 73. Therefore, the subsequent

use of the phrase "the content" elsewhere in the claims is proper.

Claim Amendments

Independent claim 1 has been amended to incorporate the limitations on the

canceled claims 7 and 8. Independent claim 37 has been amended to incorporate the

claims of canceled claims 43 and 44. And independent claim 73 has been amended to

incorporate the limitations of canceled claims 79 and 80.

Claim rejections-35 USC §102

The Examiner rejected claims 1, 2, 4-8, 37, 38, 40-44, 73, 74, and 76-80 under

35 USC §102(e) as being anticipated by Farber et al., 6,415,280 (hereinafter Farber).

The present invention discloses, methods, systems, and computer program

products for accessing information in a peer-to-peer network where each of the peer

devices is configured to store information files, and to share content from selected

information files with at least a portion of the other peer devices in the network. Each

shared file in the network has a respective fingerprint ID associated therewith relating to

its file content. According to specific embodiments, files in the peer-to-peer network

may be identified and/or accessed based upon their associated hash ID values. In this

way, it is possible to identify identical files stored in the peer-to-peer network which

have different file names and/or other metadata descriptors. Additionally, since the

content of all files having the same hash ID will be identical, an automated process may be used to retrieve the desired content from one or more of the identified files. For example, a user may elect to retrieve a desired file (having an associated hash ID) which may be stored at one or more remote locations in the peer-to-peer network. Rather than the user having to select a specific location for accessing and retrieving the desired file, an automated process may use the hash ID (associated with the desired file) to automatically select one or more remote locations for retrieving the desired file (Summary).

More specifically, independent claims 1, 37 and 73 have been amended to recite a peer-to-peer network in which a fingerprinting algorithm is used to generate a fingerprint ID relating to the contents of a file, such that files having identical content, but residing on different peer devices and having different filenames, have the same fingerprint ID. The different filenames and the fingerprint ID of the different files are stored in a database, and identified by the same fingerprint ID.

Claim 1 in part recites:

> selecting a first information file, wherein the first information file is stored at a first peer device, and has a first associated filename;
> generating, using fingerprinting algorithm, a first fingerprint ID relating to the content of the first information file;
> selecting a second information file having content identical to the first information file, wherein the second information file is stored at a second peer device, and has a has second associated filename;
> applying the fingerprinting algorithm to the content of the second information file to thereby generate an identical first fingerprint ID to that of the first information file;
> storing the first associated filename and first fingerprint ID associated with the first information file in the database system;
> storing the second associated filename and first fingerprint ID associated with the second information file in the database system; and
> identifying both the first and the second information file using the first unique fingerprint ID.

Farber fails to disclose this combination of elements. Although Farber is directed to a system for identifying and requesting data in a network using identifiers (referred to as a True Name), which are based on the contents of the data, the purpose of calculating the capture Name is to provide "a mechanism for reducing multiple copies of data items in a data processing system... which enables the identification of identical data items so as to reduce multiple copies" (col. 3, lines 11-14).

In contrast, the method and system of the present invention as claimed allows multiple copies of the same file to be stored in the network and refers to the different copies with the same fingerprint ID. Farber repeatedly teaches away from storing multiple copies of the same file, as demonstrated by the following passages:

> The purpose of this mechanism [Assimilate Data Item] is to add a given data item to the True File registry 126. If the data item already exists in the True File registry 126, this will be discovered and used during this process, and the duplicate will be eliminated. Thereby the system stores at most one copy of any data item or file by content, even when multiple names refer to the same content. (Col. 14, lines 29-35) (emphasis added).

> Further, in operation of a DP system incorporating the present invention, multiple copies of data items are avoided (unless they are required for some reason such as backups or mirror copies in a fault-tolerant system). Multiple copies of data items are avoided even when multiple names refer to the same data item. (Col. 33, lines 7-13) (emphasis added).

In support of the rejection, the Examiner repeatedly cited col. 12, lines 19-36 of Farber. In paragraph 17 of the Office Action, the Examiner cited this passage of Farber as disclosing "selecting a second information file," "the first information file," and "the content of the second information file."

However, this passage of Farber only list primitive mechanisms used to implement Farber's file system:

1. Calculate True Name; 2. Assimilate Data Item; 3. New True File; 4. Get True Name from Path; 5. Link Path to True Name; 6. Realize True File from Location; 7. Locate Remote File; 8. Make True File Local; 9. Create Scratch File; 10. Freeze Directory; 11. Expand Frozen Directory; 12. Delete True File; 13. Process Audit File Entry; 14. Begin Grooming; 15. Select For Removal; and 16. End Grooming. (Col. 12, lines 19-36)

These primitive mechanisms are provided in a file system for a data processing system, which is intended to work with an existing of operating system by augmenting some of the operating system's file management system codes (col. 6, lines 11-16). Thus, the items listed in the citation used by the Examiner are file system routines and have nothing at all to do with how files having the same content, but different names and stored on different peer devices are referred to and identified in a peer-to-peer network, as claimed in the present invention.

Nothing in Farber's description for the True Name primitive, or any other of the other primitive mechanisms, teaches or suggests "storing the first associated filename and first fingerprint ID associated with the first information file in the database system; storing the second associated filename and first fingerprint ID associated with the second information file in the database system; and identifying both the first and the second information file using the first unique fingerprint ID," as recited in claims 1, 37, and 73.

The arguments above apply with full force and effect to the remaining dependent claims because they are based on allowable independent claims. Therefore, the dependent claims are allowable for at least the same reasons as the independent claims.

In view the foregoing, it is submitted that the claims are allowable over the cited reference. Accordingly, Applicant respectfully requests reconsideration and passage to

issue of claims 1-3, 5-6, 8, 37-39, 41-42, 73-75, and 77-78 now presented.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

September 6, 2005
Date
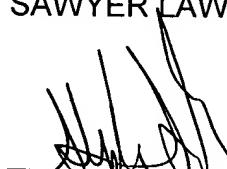
Stephen G. Sullivan
Attorney for Applicant(s)
Reg. No. 38,329
(650) 493-4540